LESSON 2 - REVIEW OF RING THEORY I

ERAN ASSAF

1. INTRODUCTION

Recall that our goal is to understand whether it is possible to find a general solution to an equation of the form $a_n x^n + \ldots + a_1 x + a_0 = 0$ (in one variable). As long as the idea was "find a solution", we didn't have to think about it much. However, once we began suspecting that there is no such formula, we need to be more careful. We need to figure out what do we mean by "general solution". Looking at the formulas for solving the quadratic, cubic and quartic equations, it seems reasonable to ask for a solution which is obtained by extracting roots and the four arithmetic operations. Abel's idea was to work in a framework where the solutions exist, and then ask whether they are of the form we want. We need to construct a framework through which we can realize which numbers can be obtained in this way. The four arithmetic operations give rise to the notion of a field, and to accommodate for extraction of roots, we will use "field extensions". However, fields are a special case of a more general structure - rings, which will be useful also for dealing with the equations themselves (polynomials). We will therefore begin with a brief review of ring theory, keeping in mind that the main applications will be polynomials and fields.

2. BASIC DEFINITIONS AND EXAMPLES

Definition 1. *A* **ring** *is a set R with two binary operations $+, \cdot$ (called addition and multiplication) such that*

- *$(R, +)$ is an abelian group.*
- *$\cdot : R \times R \to R$ is associative.*
- *$\cdot$ distributes over $+$.*

The ring R is **commutative** *if $\cdot$ is.*
The ring R has an **identity** *if there is an element $1 \in R$ which is neutral w.r.t. $\cdot$.*

Emphasize - In this class, rings will always be commutative and will always have 1.

Example 2. *The ring of integers $\mathbb{Z}$, with the usual addition and multiplication.*

Definition 3. *If R is a ring (commutative with identity), we consider formal sums*

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

with $n \geq 0$ and $a_0, \ldots a_n \in R$. $p(x)$ is called a **polynomial** *in x, with* **coefficients** *$a_0, \ldots, a_n$. If $a_n \neq 0$, we say that $f(x)$ has* **degree** *n, $a_n x^n$ is called the* **leading term** *and a_n is the* **leading coefficient**. *If $a_n = 1$, we say the $f(x)$ is* **monic**. *We call the set*

of all such polynomials the **ring of polynomials in the variable x with coefficients in R**, *and denote it by $R[x]$,*

We define addition and multiplication of polynomials as follows.

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) x^i$$

and

$$\left(\sum_{i=0}^{m} a_i x^i\right) \cdot \left(\sum_{j=0}^{n} b_j x^j\right) = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j\right) x^k.$$

Proposition 4. *$R[x]$ with the above binary operations forms a ring.*

Proof. Exercise. □

Definition 5. *A* **subring** *of R is a subgroup of R that is closed under multiplication.*

Example 6. *$\mathbb{Z}$ is a subring of $\mathbb{Q}$, which is a subring of $\mathbb{R}$.*

Example 7. *The set of constant polynomials in $R[x]$ forms a subring.*

3. Ring homomorphisms, ideals and quotient rings

Definition 8. *Let R and S be rings. A* **ring homomorphism** *is a map $\varphi : R \to S$ that preserves the binary operations.*

$$\varphi(a+b) = \varphi(a) + \varphi(b), \quad \varphi(ab) = \varphi(a)\varphi(b) \quad \forall a, b \in R.$$

The **kernel** *of φ is the set $\ker \varphi = \varphi^{-1}(0)$.*

A bijective ring homomorphism is called an **isomorphism**. *If $\varphi : R \to S$ is an isomorphism, we write $R \simeq S$, and say that they are isomorphic.*

Example 9. *The map $i_R : \mathbb{Z} \to R$ defined by*

$$i_R(n) = \underbrace{1 + 1 + \ldots + 1}_{n}, \quad i_R(-n) = -i_R(n) \quad \forall n > 0$$

is a homomorphism.

Example 10. *The natural map $\varphi : R \to R[x]$ is a ring homomorphism. Since $\ker \varphi = 0$, it is injective, and identifies R as a subring of $R[x]$. From now on, we will identify them and write $R \subseteq R[x]$.*

Example 11. *Let R be a ring, $a \in R$ an element, and consider the map $\mathrm{ev}_a : R[x] \to R$ defined by $\mathrm{ev}_a(p(x)) = p(a)$, i.e. evaluating the polynomial at a. Then ev_a is a ring homomorphism (check!), and $\ker \mathrm{ev}_a$ is the set of polynomials which have a as a root. If $a = 0$, $p(0)$ is the constant term, and $\ker \mathrm{ev}_0 = xR[x]$.*

Example 12. *Let $\varphi : R \to S$ be a ring homomorphism. We can extend it to a ring homomorphism $\widetilde{\varphi} : R[x] \to S[x]$ defined by*

$$\widetilde{\varphi}\,(a_n x^n + \ldots a_1 x + a_0) = \varphi(a_n) x^n + \ldots + \varphi(a_1) x + \varphi(a_0).$$

Definition 13. *A subgroup $I \subseteq R$ is called an* **ideal** *if it is closed under multiplication by elements of R, explicitly if for all $a \in R$, $aI \subseteq I$.*

Example 14. *In any ring R, the subgroups $\{0\}$ and R are ideals. We say that an ideal I is* **proper** *if $I \neq R$. The ideal $\{0\}$ is called* **the trivial ideal** *and is denoted by 0.*

Example 15. *For any $n \in \mathbb{Z}$, the subgroup $n\mathbb{Z}$ is an ideal in $\mathbb{Z}$, and these are all of them.*

Proposition 16. *Let $\varphi : R \to S$ be a homomorphism. Then $\ker \varphi$ is an ideal in R and $\operatorname{Im} \varphi$ is a subring of S.*

Proof. Since φ is a group homomorphism, $\ker \varphi$ is a subgroup of R, and $\operatorname{Im} \varphi$ is a subgroup of S. If $a \in R, x \in \ker \varphi$, then $\varphi(x) = 0$, so that $\varphi(ax) = \varphi(a)\varphi(x) = 0$, hence $ax \in \ker \varphi$, showing it is an ideal. If $\varphi(a), \varphi(b) \in \operatorname{Im} \varphi$, then so does $\varphi(ab) = \varphi(a)\varphi(b)$, showing that $\operatorname{Im} \varphi$ is a subring. □

Example 17. *Consider the map i_R. Its kernel is an ideal in $\mathbb{Z}$, so it has to be $n\mathbb{Z}$.*

Proposition 18. *If I, J are ideals in R, so are $I \cap J$ and $I + J$. If $\{I_\alpha\}_{\alpha \in A}$ are ideals, then so is $I = \bigcap_{\alpha \in A} I_\alpha$.*

Proof. Start with the last statement. I is a subgroup of R, and if $a \in R$, $x \in I$, then for all α, $x \in I_\alpha$ hence $ax \in I_\alpha \subseteq I$. Thus, $ax \in I$ and $aI \subseteq I$. Then $I \cap J$ is a special case, $I + J$ is a subgroup and $a(I + J) = aI + aJ \subseteq I + J$. □

Definition 19. *Let $S \subseteq R$ be a subset. Then* **the ideal generated by** *S, $I = \langle S \rangle$, is the minimal ideal containing S. If $S = \{a_1, \ldots, a_n\}$ is finite, we write $I = (a_1, \ldots, a_n)$. We write IJ for the ideal generated by the products*

$$IJ = \langle \{ab : a \in I, b \in J\} \rangle = \left\{ \sum a_i b_i : a_i \in I, b_i \in J \right\}.$$

Proposition 20. *Let I be an ideal of R, then the quotient group R/I forms a ring with the binary operations*

$$(a + I) + (b + I) = (a + b) + I, \quad (a + I) \cdot (b + I) = ab + I \quad \forall a, b \in R.$$

It is called the **quotient ring**.

Proof. Since I is a (normal) subgroup of the abelian group $(R, +)$, $(R/I, +)$ is an abelian group. The multiplication is well defined, since if $a_1, a_2, b_1, b_2 \in R$ are such that $a_1 + I = a_2 + I$ and $b_1 + I = b_2 + I$, then $a_1 - a_2, b_1 - b_2 \in I$, and as I is an ideal in R, also (using distributivity in R)

$$a_1 b_1 - a_2 b_2 = (a_1 - a_2)b_1 + a_2(b_1 - b_2) \in I \implies a_1 b_1 + I = a_2 b_2 + I.$$

Since $\cdot : R \times R \to R$ is associative, we have

$$[(a + I)(b + i)](c + I) = (ab)c + I = a(bc) + I = (a + I)[(b + I)(c + I)],$$

for any $a, b, c \in R$, establishing associativity in R/I. The distributivity law in R also yields

$$(a+I)[(b+i)+(c+I)] = a(b+c)+I = (ab+ac)+I = (ab+I)+(ac+I) = (a+I)(b+I)+(a+I)(c+I),$$

for any $a, b, c \in R$, showing that R/I is a ring.

As R is commutative, we also have $(a+I)(b+I) = ab+I = ba+I = (b+I)(a+I)$ for any $a, b \in R$ so that R/I is commutative, and finally note that $(a+I)(1+I) = a+I$ for all $a \in R$, so that $1+I$ is an identity in R/I. □

Theorem 21 (The First Isomorphism Theorem for Rings)**.** *If $\varphi : R \to S$ is a ring homomorphism, then $R/\ker\varphi \simeq \varphi(R)$.*

For any ideal I in R, the natural map $R \to R/I$ is surjective with kernel I.

Proof. Since φ is a homomorphism of abelian groups, $\ker\varphi$ is a (normal) subgroup of the abelian group $(R, +)$, and by the first isomorphism theorem for groups, we know that $R/\ker\varphi \simeq \varphi(R)$ as abelian groups, via the isomorphism $\overline{\varphi}(a + \ker\varphi) = \varphi(a)$. Because φ is a ring homomorphism, for any $a, b \in R$ we have

$$\overline{\varphi}((a+\ker\varphi)(b+\ker\varphi)) = \overline{\varphi}(ab+\ker\varphi) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(a+\ker\varphi)\overline{\varphi}(b+\ker\varphi),$$

so that $\overline{\varphi}$ is also a ring homomorphism, hence an isomorphism of rings. For the second statement, note that $a \mapsto a + I$ for all $a \in R$, showing surjectivity, and that $a + I = I$ iff $a \in I$. □

Example 22. *The natural map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is called* **reduction mod** *n.*

Example 23. *Consider the map $\mathrm{ev}_0 : R[x] \to R$. Then $\mathrm{ev}_0(R[x]) = R$, and $\ker \mathrm{ev}_0 = (x)$. Therefore, $R[x]/(x) \simeq R$.*

4. Fields and integral domains

Definition 24. *A ring F (commutative, with 1) is called a* **field** *if $(F\backslash\{0\}, \cdot)$ is a group.*

Example 25. *The rationals $\mathbb{Q}$, as well as the real and complex numbers, $\mathbb{R}$ and $\mathbb{C}$.*

Proposition 26. *Let $D \in \mathbb{Q}$ be a non-square, and define*

$$\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\} \subset \mathbb{C}.$$

Then $\mathbb{Q}(\sqrt{D})$ is a field (called a **quadratic field***).*

Proof. Exercise. □

Definition 27. *An element $0 \neq a \in R$ is called a* **zero divisor** *if there exists $0 \neq b \in R$ such that $ab = 0$. An element $u \in R$ is called a* **unit** *is there exists $v \in R$ such that $uv = 1$. We denote $v = u^{-1}$.*

Proposition 28. *The set of units in R form a group.*

Proof. $(uv)v^{-1}u^{-1} = 1$. □

Definition 29. *The set of units in R is called the* **unit group** *of R and is denoted by $R^\times$.*

Example 30. $\mathbb{Z}^\times = \{\pm 1\}$.

Example 31. *A ring F is a field iff $F^\times = F\backslash\{0\}$, i.e. every nonzero element is a unit.*

Corollary 32. *A ring F is a field $\iff$ its only ideals are 0 and F.*

Proof. If F is a field and $I \neq 0$, let $0 \neq a \in I$. Then $1 = a^{-1}a \in I$, so $I = F$. Conversely, let $0 \neq a \in F$, then the ideal $(a) \neq 0$ must be F, so $1 \in F = (a)$, hence there exists $a^{-1} \in F$ such that $1 = aa^{-1}$, so that F is a field. □

Corollary 33. *If $\varphi : F \to R$ is a homomorphism from a field, then it is either zero or injective.*

Proof. $\ker \varphi$ is an ideal in F, hence either F or 0. □

Definition 34. *A ring R is called an* **integral domain** *if it has no zero divisors.*

Example 35. *$\mathbb{Z}$ is an integral domain.*

Example 36. *$\mathbb{Z}/n\mathbb{Z}$ is an integral domain $\iff$ n is prime.*

Example 37. *A subring of an integral domain is an integral domain.*

Proposition 38. *Any field F is an integral domain.*

Proof. If $0 \neq a \in F$, and $b \in F$ is such that $ab = 0$, then $b = a^{-1}(ab) = 0$. □

Proposition 39. *For an integral domain R, the following statements hold.*

1. $\deg p(x)q(x) = \deg p(x) + \deg q(x)$ *for any nonzero* $p(x), q(x) \in R[x]$.
2. $R[x]$ *is an integral domain.*
3. $R[x]^\times = R^\times$.

Proof. Let $a_m x^m$ and $b_n x^n$ be the leading terms of $p(x), q(x)$ respectively. Then $p(x)q(x) = a_m b_n x^{m+n} + \sum_{j<m+n} c_j x^j$. Since R is an integral domain and $a_m, b_n \in R$ are nonzero, $a_m b_n \neq 0$ so the leading term of $p(x)q(x)$ is $a_m b_n x^{m+n}$, showing (1) and (2). Finally, if $p(x) \in R[x]^\times$, then there is $q(x) \in R[x]$ such that $p(x)q(x) = 1$, hence (as both are nonzero)

$$0 = \deg 1 = \deg p(x)q(x) = \deg p(x) + \deg q(x),$$

so $\deg p(x) = \deg q(x) = 0$, showing that $p(x), q(x) \in R$, hence in $R^\times$, proving (3). □

5. SUMMARY

We have reviewed the notions of a ring, a ring homomorphism and ideals. We have seen that ring homomorphisms can be extended to the polynomial rings, and that every ring R carries a (unique) homomorphism $i_R : \mathbb{Z} \to R$. We defined fields and integral domains, saw that a homomorphism from a field is injective, and that the polynomial ring over an integral domain form themselves an integral domain.